REMARKS/ARGUMENTS

Reconsideration is respectfully requested.

Claims 1-12 are pending before this amendment. By the present amendment, claims 1, 3, 5, 9, and 11 are amended. No new matter has been added.

In the office action (page 2), claims 1, 3, 5, 9 and 11 stand rejected under 35 U.S.C. §112 as there is insufficient antecedent basis for the recited limitation "the add-round-key generation unit" and to correct the 128-bit data not being input into the round key generation unit. In response, the applicants have amended the claims to as suggested by the examiner, which is respectfully appreciated. More specifically, the amended claims 1, 3, 5, 9, and 11 now recite inter alia: --wherein the round keys generated in the ~~add-round-key~~ round key generation unit is added to an upper M/m input data in the round operation execution-- and --wherein the end stage of every round indicates that the data in the unit of M/m bits (where m is 2, 3 or 4) have been processed in all of the at least transforms of the substitution, mixcolumn and add-round-key~~, and a round key generation in the round operation execution unit~~--. Therefore, the applicants respectfully requested withdrawal of the §112, ¶2 rejection.

In the office action (page 3), claims 1-8 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Publication No. 2002/0131588 (Yang) in view of U.S. Patent No. 6,246,768 (Kim).

The applicants respectfully disagree.

The present invention relates to a rijndael block cipher apparatus including an operational unit for efficiently performing a round operation for encrypting/decrypting the

rijndael block cipher, where the rijndael block cipher apparatus is made to mount in a mobile terminal such as a cellar phone and a PDA or a smart card, which requires a high-rate and small-sized cipher processor, and which can encrypt and decrypt important data that requires security at high speed (specification page 2 [11] and [12]). The rijndael block cipher apparatus uses the rijndael algorithm that require a number or round where the number of rounds performed for the rijndael block cipher apparatus is determined by the number of bits used by the round keys (specification page 1 [7]).

The rijndael algorithm of the present invention supports a variable block length of an SPN (Substitution-Permutation Network) structure, and enables the use of 128-bit, 192-bit, and 256-bit keys with respect to the respective block lengths (specification page 1 [7]).

The key lengths determine the number of rounds in the rijndael algorithm, where the 128-bit keys recommend using 10 rounds and the192-bit and 256-bit keys use 12 and 14 rounds respectively. For example, the present invention discloses a rijndael algorithm using a 128-bit key that **reduces hardware implementation** of the rijndael algorithm over the prior art. Typically, the rijndael algorithm encrypts/decrypts data for the rijndael block encryption/decryption by repeating round operations where a round operation for the encryption process of the rijndael block cipher is composed of four transforms of substitution, shift_row, mixcolumn and add-round-key, and a round operation for the decryption process is composed of four transforms of inverse-shift_row, inverse substitution, add-round-key and inverse mixcolumn. As a result, the times required for the round operation for the rijndael block cipher and hardware resources is vital to the performance of a rijndael cipher processor for cellar phone and a PDA or a

smart card, which requires a high-rate and small-sized cipher processor (specification pages 1 and 2 [9] [10]).

The present invention **reduces the hardware** by transforming the 128-bit input key into a 128-bit round key for encryption/decryption by dividing the 128-bit input data into upper 64 bits and lower 64 bits and **simultaneously** performing the round operations for each the upper and lower 64 bits of input data. For example, the upper 64-bit data is added with the upper 64-bit round key generated by the round key generation unit while **simultaneously performing a mixcolumn of the lower 64-bit data.**

That is, the rijndael algorithm of the present invention discloses encrypting/decrypting the divided data (i.e.; upper and lower 64-bit data) for the rijndael block encryption/decryption by repeating round operations where a round operation for the encryption process of the rijndael block cipher is composed of four transforms of substitution, shift_row, mixcolumn and add-round-key, and a round operation for the decryption process is composed of four transforms of inverse-shift_row, inverse substitution, add-round-key and inverse mixcolumn where different transforms of the divided data are **simultaneously** performed in the **same manner with the same circuit design for each of the four transforms** but on different transforms (i.e.; where both of the upper and lower input data are acted on by the same transform circuit) by the upper and lower input data bits at the same time (**same clock cycle**), which is performed **before** the end of each round to generate the encrypted/decrypted data of 128, 192, or 256 bits respectively to/from a cellar phone and a PDA or a smart card that require high-rate and small-sized cipher processor (specification page 8 [18]).

Claim 1 has been amended to clarify this aspect of the present invention. Claim 1 now recites, inter alia:

> --wherein the round keys generated in the ~~add-round-key~~ **round key** generation unit is added to an upper M/m input data in the round operation execution unit while simultaneously begin processing of a lower M/m input data in the round operation execution unit before the end stage of every round for the upper M/m input data in the round operation execution unit **at a same clock cycle without the upper M/m input data and the lower M/m input being processed in any one of a same transform of the transforms comprising of at least the substitution, mixcolumn and add-round-key**,
>
> wherein the end stage of every round indicates that the data in the unit of M/m bits (where m is 2, 3 or 4) have been processed in all of the at least transforms of the substitution, mixcolumn and add-round-key~~, and a round key generation in the round operation execution unit~~, **and**
>
> **wherein the processing of the upper M/m input data and the lower M/m input data are transformed in a same manner of a same circuit for each of the at least transforms of the substitution, mixcolumn and add-round-key**--.

Nowhere does Yang and/or Kim, alone or in combination, teach or suggest amended claim 1 of the present invention, and one skilled in the art would not have been motivated at the time the invention was made to modify the cited references to produce the claimed invention.

In contrast and understood by the examiner, where the examiner states Kim disclosing in FIG. 2, reference number 522, and 524, and col. 3, lines 46-62, "in the first key adding circuit, key SK1 adds to divided upper half data X1, **at the same time**, key SK2 adds to divide lower half data X2 before the end of four processing stages" (OA page 5, last 5 lines), where X1 and X2 data have their own separates circuits for each of their respective stages that can not be executed simultaneously in a same circuit for both the X1 and X2 data for a same clock cycle at different stages. That is, FIG. 2 of Kim discloses a first and second division units where data X divides the 64 bits into two

separate 32 bit (X1 and X2) **that are each operated on by different circuits at the same time**. Accordingly, nowhere in Kim are the divided data operated on by the same circuits in a same manner during a same clock cycle but at different stages, which must be done before the end stage of every round of either of the divided data X1 or X2.

In contradistinction, the present invention discloses performing the transform of add round key to the upper 64-bit while simultaneously performing the transformation of a mixcolumn on the lower 64-bit data during the same clock cycle. That is, the rijndael block cipher apparatus of the present invention performs all round operations for encrypting and decrypting input data for rijndael block encryption/decryption in the unit of 64 bits (upper and lower 64-bit data), and to generate round keys required for the round operations of the upper 64-bit data "**simultaneously**" with performing the transformation of mixcolumn of the round operations for lower 64-bit data (specification [33], [89], [102], [110], [111], and [116]. In the present invention, the round keys generated in the round key generation unit is added to an upper M/m input data in the round operation execution unit while **simultaneously** beginning processing of a lower M/m input data in the round operation execution unit before the end stage of every round for the upper M/m input data in the round operation execution unit at **a same clock cycle** without the upper M/m input data and the lower M/m input being processed in any one of a same transform of the transforms comprising of at least the substitution, mixcolumn and add-round-key such that the processing of the upper M/m input data and the lower M/m input data are transformed in a same manner of a same circuit for each of the at least transforms of the substitution, mixcolumn and add-round-key (specification at least at [111] and FIG. 2). The end stage of every round of the present

invention occurs when the data in the unit of M/m bits (where m is 2, 3 or 4) have been processed in all of the at least transforms of the substitution, mixcolumn and add-round-key.

Accordingly, neither Yang nor Kim, whether considered alone or in combination, teaches nor suggests amended claim 1 of the present invention, which recites, inter alia: --wherein the round keys generated in the round key generation unit is added to an upper M/m input data in the round operation execution unit while simultaneously begin processing of a lower M/m input data in the round operation execution unit before the end stage of every round for the upper M/m input data in the round operation execution unit at a same clock cycle without the upper M/m input data and the lower M/m input being processed in any one of a same transform of the transforms comprising of at least the substitution, mixcolumn and add-round-key, wherein the end stage of every round indicates that the data in the unit of M/m bits (where m is 2, 3 or 4) have been processed in all of the at least transforms of the substitution, mixcolumn and add-round-key, and wherein the processing of the upper M/m input data and the lower M/m input data are transformed in a same manner of a same circuit for each of the at least transforms of the substitution, mixcolumn and add-round-key--. Also, one skilled in the art would not have been motivated at the time the invention was made to modify the cited references to produce the claimed invention.

Therefore, an indication of allowable subject matter with respect to claim 1 is respectfully requested.

As to claim 2, the applicants respectfully submit that claim 2 is allowable at least since it depends from claim 1, which is now considered to be in condition for allowance

for the reasons mentioned above for claim 1.

Independent amended claims 3 and 5 recite similar features to those found in claim 1. Therefore, for reasons analogous to those argued above with respect to claim 1, amended claims 3 and 5 are patentable over the applied references.

As to claims 4 and 6-8, the applicants respectfully submit that these claims are allowable at least since they depend from either claim 3 or claim 5, which are now considered to be in condition for allowance for the reasons mentioned above for claim 1.

In the office action (page 15), claims 9-10 [where we believe the examiner also meant claims 11-12] stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yang, in view of U.S. Patent No. 6,230,257 (Roussel) and further in view of Kim. The "et al." suffix is omitted in a reference name.

Applicants respectfully traverse this rejection because Roussel either alone or in combination with Yang and/or Kim fails to disclose or suggest all of the claim limitations of either claim 9 or claim 11 as mentioned above for claim 1, where claims 9 and 11 recite similar features to those found in claim 1.

As to claims 10 and 12, the applicants respectfully submit that claims 10 and 12 allowable at least since they depend from either claim 9 or claim 11, which are now considered to be in condition for allowance for the reasons mentioned above for claim 1.

For the reasons set forth above, the applicants respectfully submit that claims 1-12, now pending in this application, are in condition for allowance over the cited references. Accordingly, the applicants respectfully request reconsideration and withdrawal of the outstanding rejections and earnestly solicit an indication of allowable

subject matter.

This amendment is considered to be responsive to all points raised in the office action. Should the examiner have any remaining questions or concerns, the examiner is encouraged to contact the undersigned attorney by telephone to expeditiously resolve such concerns.

Respectfully submitted,

Dated: August 25, 2009

Keith S. Van Duyne

Keith S. Van Duyne, Reg. No. 54,505
Ladas & Parry LLP
224 South Michigan Avenue
Chicago, Illinois 60604
(312) 427-1300